User Guide

www.tenda.cn

W300D Wireless-N
ADSL2+ Modem Router

Copyright Statement

is the registered trademark of Shenzhen Tenda Technology Co., Ltd. All the products and product names mentioned herein are the trademarks or registered trademarks of their respective holders. Copyright of the whole product as integration, including its accessories and software, belongs to Shenzhen Tenda Technology Co., Ltd. Without the permission of Shenzhen Tenda Technology Co., Ltd, any individual or party is not allowed to copy, plagiarize, imitate or translate it into other languages. All the photos and product specifications mentioned in this manual are for references only. As the upgrade of software and hardware, there will be changes. And if there are changes, Tenda is not responsible for informing in advance. If you want to know more about our product information, please visit our website at www.tenda.cn.

Content

Chapter 1：Product Overview 1

1.1 Product Introduction 1
1.2 Product Features 2
1.3 Package Contents 4

Chapter 2：Getting to Know the Router 5

2.1 Rear Panel and Port Description 5
2.2 Front Panel and LED Description 6
2.3 Hardware Installation 7

Chapter 3：Getting to Connect the Broadband Router 10

3.1 How to Set the Network Configurations for My Computer 10
3.2 How to Check the Network Connection 14
3.3 How to Access the Web-based Configuration Utility 15

Chapter 4：DSL Setting 17

4.1 DSL Setting 17

Chapter 5：Advanced Setting 29

5.1 LAN Setting 29
5.2 MAC Address Clone 30
5.3 DNS Settings 32

Chapter 6：Wireless Settings 33

6.1 Basic Setting 33
6.2 Wireless Security Settings 36
6.2.1 Mixed WEP 36
6.2.2 WPA- Personal 38

6.2.3 WPA2-Personal 39
6.2.4 WPA-Enterprise..... 40
6.2.5 WPA2-Enterprise..... 41
6.2.6 802.1X Authentication 42
6.3 WPS Setting..... 44
6.4 WDS Setting 46
6.5 Advanced Wireless Setting 48
6.6 Wireless Access Control 50
6.7 Wireless Connection Status 51

Chapter 7：DHCP Server 52

7.1 DHCP Server Setting 52
7.2 DHCP Client List..... 53

Chapter 8：Virtual Server 54

8.1 Single Port Forwarding..... 54
8.2 Port Range Forwarding..... 57
8.3 Port Trigger Setting 59
8.5 DMZ Host 63
8.6 UPnP Setting 64

Chapter 9: Traffic Control 65

Chapter 10：Security Setting 67

10.1 Client Filter Settings 67
10.2 URL Filter..... 69
10.3 MAC Address Filter 71
10.4 Prevent Network Attack..... 73
10.5 Remote Web Management 74
10.6 Local Web Management..... 76
10.7 WAN Ping..... 78

Chapter 11: Routing Setting..... 79

11.1 Routing Table..... 79
11.2 Static Routing..... 80

Chapter 12: System Tools 82

12.1 Time Setting 82
12.2 DDNS 84
12.3 Backup/Restore Setting 85
12.4 Firmware Upgrade 87
12.5 Restore to Factory Default Settings 89
12.6 Reboot 90
12.7 Password Change 91
12.8 System Log 92

Appendix I: Glossary 93

Chapter 1：Product Overview

1.1 Product Introduction

W300D ADSL2+ 300M Wireless Broadband Router provides up to 24Mbps downstream rate and 1Mbps upstream rate, which integrates ADSL2+ Modem, wireless router, four-port LAN switch and firewall in one. W300D utilizes advanced MIMO technology and increases over 8 times of transmission range of ordinary 802.11g products. Compatible with IEEE802.11n (Draft 2.0) and IEEE802.11g/b standards, it can provide up to 300Mbps stable transmission rate.

It supports WDS (Wireless Distribution System) function for repeating and amplifying the signals to extend the wireless network coverage. Besides, it can disable SSID broadcast manually. WPS (PBC and PIN) encryption method, port filtering and MAC address filtering can protect your network from malicious attack. W300D can be managed through local/remote Web management interface anywhere. Moreover, the

WMM function can make your voice and video smoother. Powerful and exquisite, it is the best choice for SOHOs and small-sized enterprises to share the wireless network.

1.2 Product Features

- Integrates ADSL2+ Modem, wireless router, four-port LAN switch and firewall
- Complies with IEEE802.11n (Draft 2.0), compatible with IEEE802.11b and IEEE802.11g standards
- MIMO technology utilizes reflection signals to increase 8 times transmission distance of original 802.11g standard and reduces the "dead spots" in the wireless coverage area
- Provides 300Mbps receiving rate and 300Mbps sending rate
- Supports WMM to make your voice and video more smooth
- Supports 64/128-bit WEP, WPA, WPA2 encryption methods and 802.1x security authentication standard
- Supports ATM Forum UNI 3.0, 3.1 and 4.0

Permanent Virtual Circuits standard

- Setup Wizard support for fast and easy configurations
- WPS (PBC and PIN) encryption method to free you from remembering long passwords
- Supports remote/local Web management
- Supports wireless Roaming technology to ensure high-efficient wireless connections
- Supports wireless SSID stealth mode and MAC address access control
- Supports Auto MDI/MDIX
- Provides system log to record the status of the router
- Supports MAC address filtering, IP address filtering, URL filtering and NAT rules
- Supports UPnP and DDNS
- Supports access control over 30 MAC address entries
- Supports DHCP server/client
- Supports SNTP
- Supports virtual server and DMZ host
- Supports bandwidth control based on IP address range
- Built-in firewall to prevent hacker attack

- Supports auto wireless channel selection
- Supports WDS function (Wireless Distribution System)

1.3 Package Contents

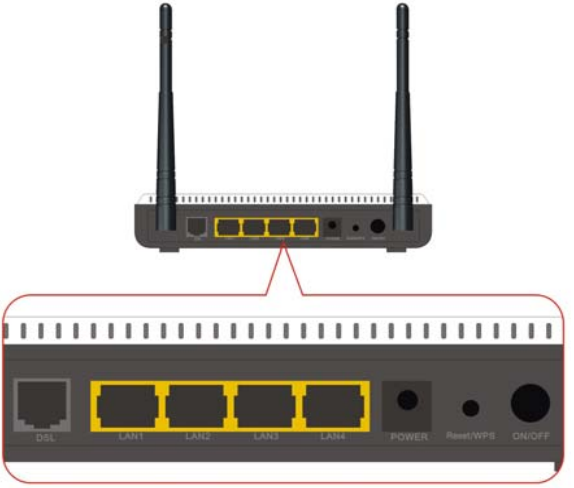
- One W300D Wireless-N ADSL2+ Broadband Router
- One CD-ROM (User Guide, Setup Wizard, etc.)
- One Quick Installation Guide
- Two RJ11 Telephone Lines
- One RJ45 Ethernet Cable
- One Power Adapter
- One Voice Splitter

If any of listed items are missing or damaged, please contact the Tenda reseller from whom you purchased for replacement immediately.

Chapter 2：Getting to Know the Router

2.1 Rear Panel and Port Description

Rear Panel View：



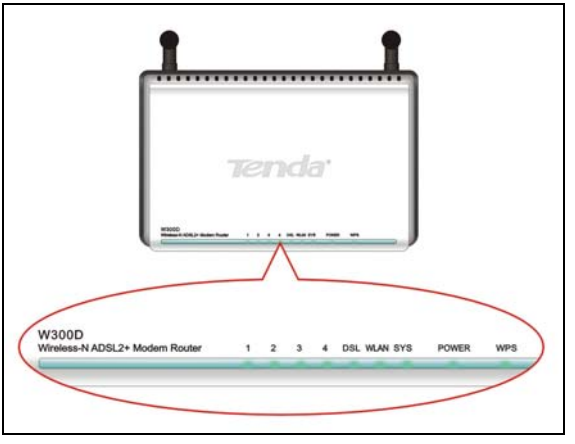
Rear Panel Description：

Rear Panel Interface	Description
LAN(1-4)	Connect with your computer's NIC or uplink to hub or switch.

RESET/WPS	Note: press this button for 7 seconds, the settings you configured will be deleted and restored to factory default setting. If press for 1 second, the WPS (PBC) is enabled.
DSL	Connect with DSL telephone line.
POWER	For AC12/1.0A connection

2.2 Front Panel and LED Description

Some LED indicators on the front panel of W300D are located here, shown as below:

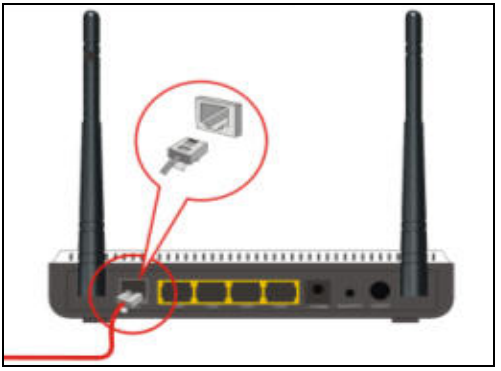


LED Indicator	State	Description
POWER	Always ON	Indicates it is powered on well.
SYS	Blinking	Indicates the system works on well.
DSL	Always ON	Indicates it is connected with DSL termination well.
	Blinking	Indicates it is going on connection negotiation
WLAN	Always ON	Indicates the wireless module works well.
	Blinking	Indicates it is transmitting and/or receiving data.
LAN(1/2/3/4)	Always ON	Indicates it is connected well.
	Blinking	Indicates the router's LAN port is transmitting and/or receiving data.
WPS	Blinking	Indicates the Router is negotiating with WPS clients in WPS Mode.

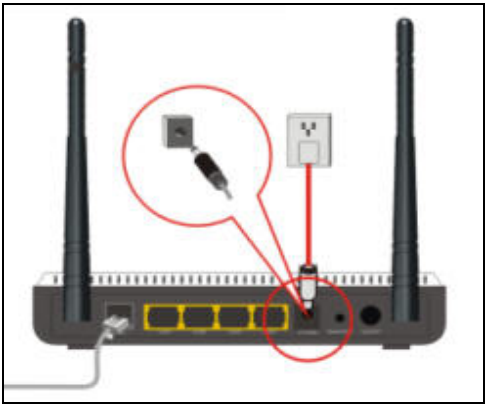
2.3 Hardware Installation

Before the Router's setting, please follow the next steps to connect with. For better wireless performance, please locate the Router in the center of wireless coverage.

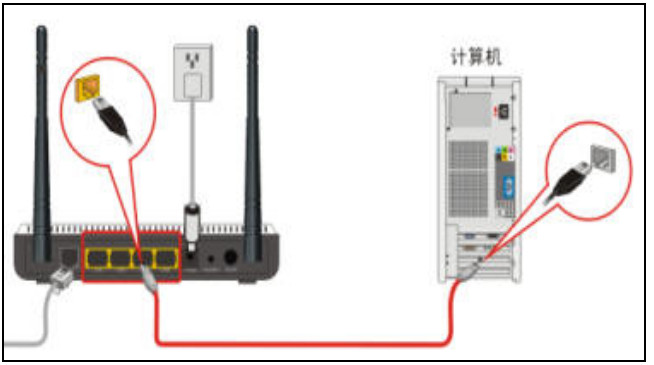
1. Connect to the Router's DSL port with telephone line.



2. Use the delivery-attached power adapter to power the Router.



3. Connect the LAN port of the Router to the network adapter of your computer with one cable.



IMPORTANT:

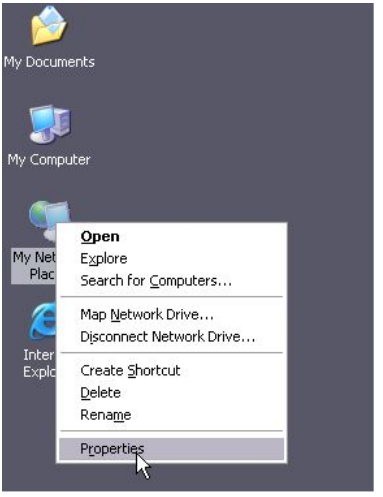
Please use the included power adapter. Use of a different power adapter could cause damage and void the warranty for this product.

Chapter 3: Getting to Connect the Broadband Router

For easy and fast configuration, the following steps for network configuration are required.

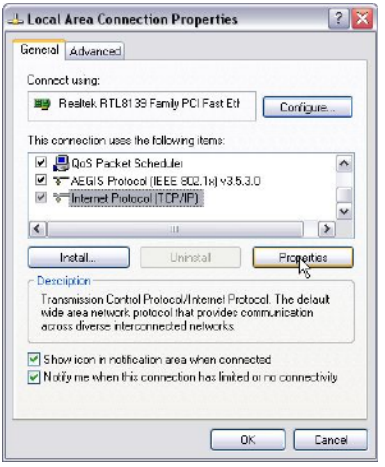
3.1 How to Set the Network Configurations for My Computer

1. Right click “My Network Places” and select “Properties”.

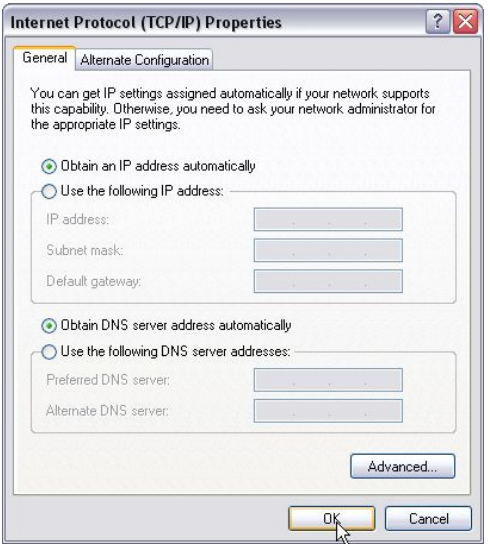


2. Right click “Local Area Network Connection” and select “Properties”.

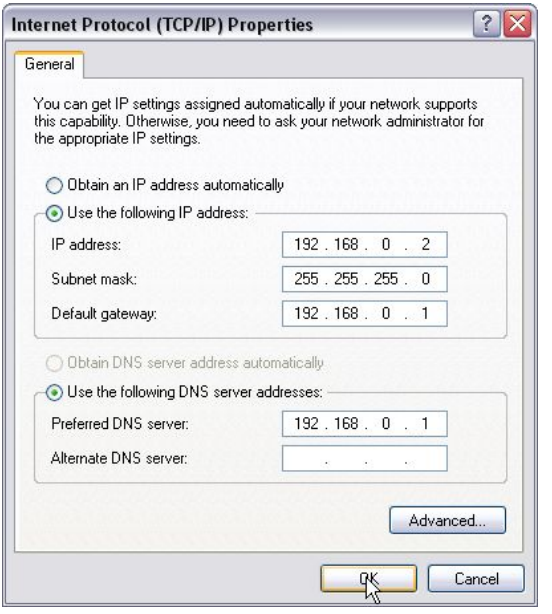
3. Select “Internet Protocol (TCP/IP)” and click “Properties”.



4. Select “Obtain an IP address automatically” and “Obtain DNS server address automatically”. Click “OK” to save the configurations.


Internet Protocol (TCP/IP) Properties
General
Alternate Configuration
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
Subnet mask:
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

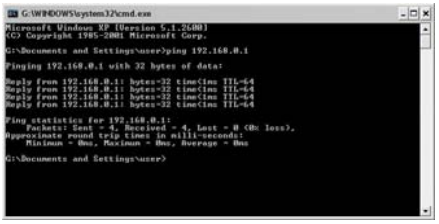
Or select “Use the following IP address” and enter the IP address, Subnet mask, Default gateway as shown right. Of course, you need to input the DNS server address provided by your ISP. Otherwise, you can use the Router’s default gateway as the DNS proxy server. Click “OK” to save the configurations.


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 192 . 168 . 0 . 2
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 192 . 168 . 0 . 1
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server: 192 . 168 . 0 . 1
Alternate DNS server:
Advanced...
OK
Cancel

3.2 How to Check the Network Connection

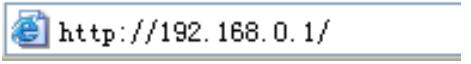
1. Select Start"—"Programs"—"Accessories" —"Command Prompt".

2. Input the "ping 192.168.0.1" and press "Enter". If the screen displays as the right figure, it means your PC is connected to your router successfully. If not, please make sure the hardware installation and network adapter are OK.


G:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
G:\Documents and Settings\user>ping 192.168.0.1
Pinging 192.168.0.1 with 32 bytes of data:
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Reply from 192.168.0.1: bytes=32 time<1ms TTL=64
Ping statistics for 192.168.0.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
G:\Documents and Settings\user>

3.3 How to Access the Web-based Configuration Utility

1. To access the Router's Web-based Utility, launch a web browser such as Internet Explorer or Firefox and enter the Router's default IP address, http://192.168.0.1. Press "Enter".



2、input the "admin" in both User Name and Password. Click "OK".

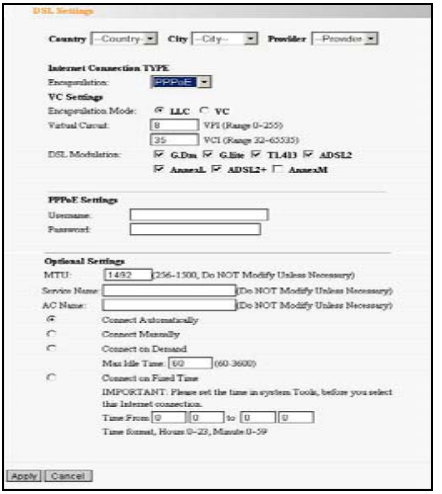
3、If you enter the correct user name and password, the following page appears.

Chapter 4：DSL Setting

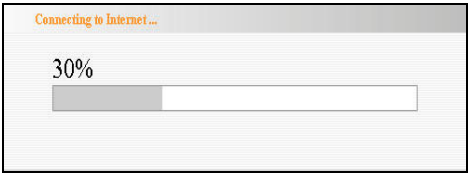
This section deals with how to configure the Router's basic setting via Web interface.

4.1 DSL Setting

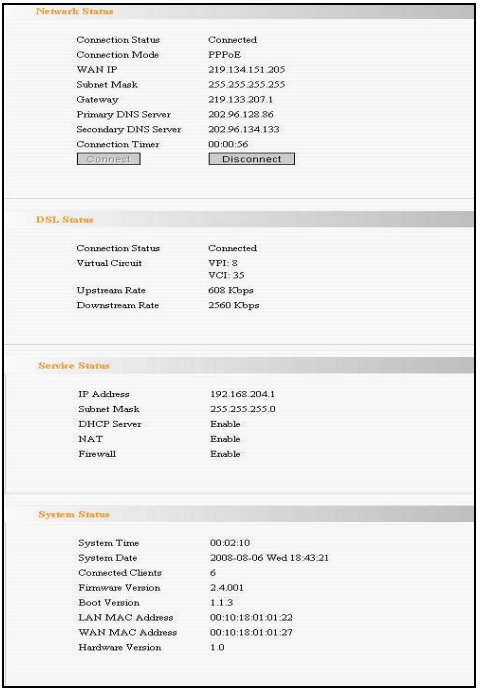
This guide can assist you to configure the Router's connection mode and basic parameters fast. The Router supports five common connection modes (Bridging, MER, IpoA, PPPoE, PPPoA). Select one according your actual requirements.


DSL Settings
Country --Country-- City --City-- Provider --Provider--
Internet Connection TYPE
Encapsulation: PPPoE
VC Settings
Encapsulation Mode: LLC VC
Virtual Circuit: 8 VPI (Range 0~255)
35 VCI (Range 32~65535)
DSL Modulation: G.Dmt G.lite T1.413 ADSL2
AnnexL ADSL2+ AnnexM
PPPoE Settings
Username:
Password:
Optional Settings
MTU: 1492 (256-1500, Do NOT Modify Unless Necessary)
Service Name: (Do NOT Modify Unless Necessary)
AC Name: (Do NOT Modify Unless Necessary)
Connect Automatically
Connect Manually
Connect on Demand
Max Idle Time: 60 (60-3600)
Connect on Fixed Time
IMPORTANT: Please set the time in system Tools, before you select this Internet connection.
Time From: 0 0 to 0 0
Time format, Hours 0~23, Minute 0~59
Apply Cancel

After the setting is completed, please click “Apply”. The device will reboot and the settings will go into effect.



The device’s status will be refreshed in the following page:



Network Status:

Connection State:

To check if it is connected well with ISP

Connection Mode:

Show the connection mode for Internet access.

WAN IP、Subnet Mask、Gateway、Primary DNS Server、Secondary DNS Server:

After the Router connects well with ISP, the TCP/IP parameters are obtained. Or you can specify by manual.

Connection Time:

The communication time for the Router and ISP

DSL State:

Connection State:

Show If the DSL is connected well.

Virtual Circuit:

Show the VPI/VCI value.

Upstream Rate:

The upstream rate resulted from the negotiation between DSL and ISP.

Downstream Rate:

The downstream rate resulted from the negotiation between DSL and ISP.

Server State:

IP Address:

The IP address for the Router's Web interface login.

DHCP Server、NAT、Firewall:

Enable or disable.

System Status:

System Time:

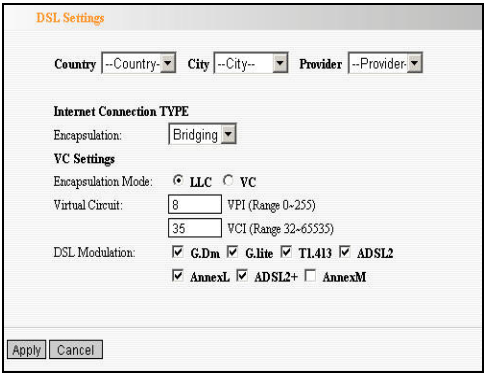
The running time of the Router.

System Date:
The system date of the Router
Client: The client number connected with the device

➔Connection Mode 1: Bridging

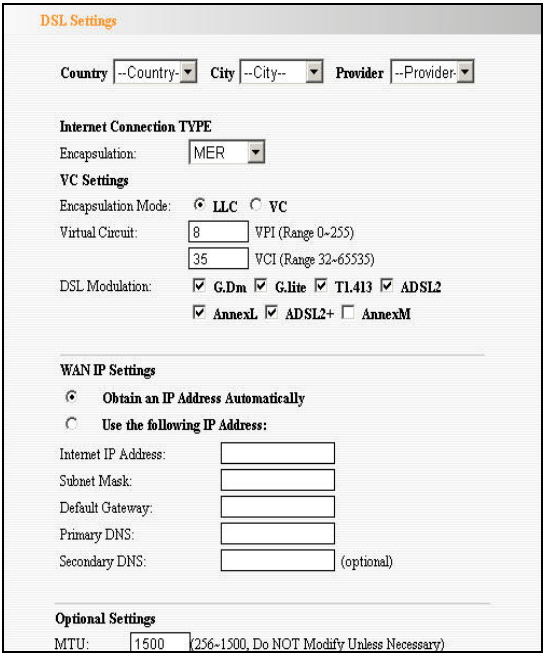
If you want to configure the device's connection mode as Bridging, please select "Bridging" in the Encapsulation field under Internet Connection Mode.

Region selection: Country, City, Provider. If the city or ISP is not listed in the drop-down menu, you can enter the VPI and VCI value. "Encapsulation Mode", "DSL Modulation" are suggested to select the default value. If there is something wrong, you can inquire your local ISP.



➔Connection Mode 2：MER

If your ISP provides your connection way as Dynamic IP (it means you obtain different IP address each time to access the Internet), select “MER” in “Encapsulation” field and “Auto obtain IP address” in “WAN IP setting”.



Region selection: Country, City, Provider. If the city or ISP is not listed in the drop-down menu, you can enter the VPI and VCI value. “Encapsulation Mode”, “DSL Modulation” are suggested to select the default value. If there is something wrong, you can inquire your local ISP.

If your ISP provides your connection way as Dynamic IP (it means you obtain different IP address each time to access the Internet), select “MER” in “Encapsulation” field and “Use the following IP address” in “WAN IP setting”. You need input the “IP address”, “Subnet Mask”, “Default Gateway”, “DNS Server”, “Secondary DNS Server” into the corresponding fields.

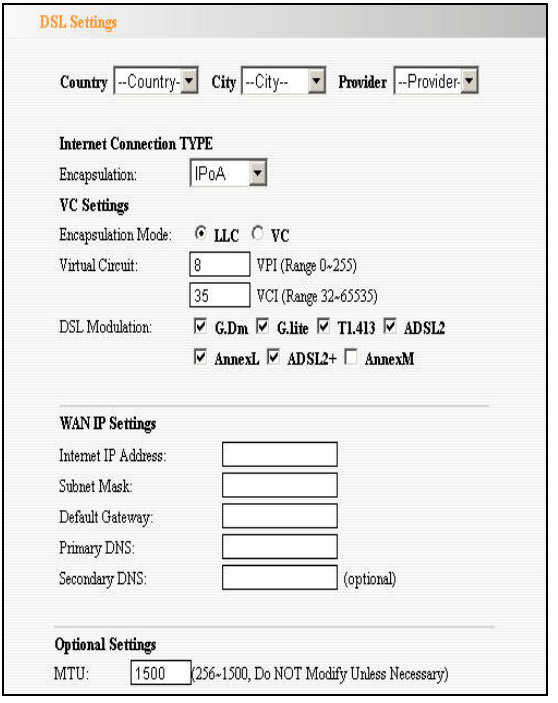
Other Settings:

MTU:

Maximum Transmission Unit. The default value is 1500. Don’t modify the default value unless necessary.

➔Connection Mode 3：IPoA

If your ISP provides your connection way as IPoA, select “IPoA” in “Encapsulation” field. You need input the “IP address”, “Subnet Mask”, “Default Gateway”, “DNS Server”, and “Secondary DNS Server” into the corresponding fields.



Region selection: Country, City, Provider. If the city or ISP is not listed in the drop-down menu, you can enter the VPI and VCI value. “Encapsulation Mode”, “DSL Modulation” are suggested to select the default value. If there is something wrong, you can inquire your local ISP.

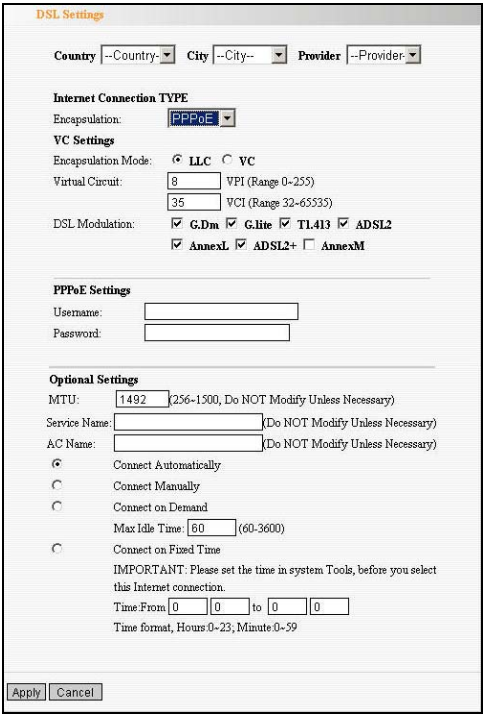
Other Settings:

MTU:

Maximum Transmission Unit. The default value is 1492. Don’t modify the default value unless necessary.

➔Connection Mode 4：PPPoE

If your ISP provides your connection way as PPPoE, select “PPPoE” in “Encapsulation” field. You need input your user name and password provided by ISP or network administrator in “PPPoE Setting” corresponding fields.



Region selection: Country, City, Provider. If the city or ISP is not listed in the drop-down menu, you can enter the VPI and VCI value. “Encapsulation Mode”, “DSL Modulation” are suggested to select the default value. If there is something wrong, you can inquire your local ISP.

Other Settings:

MTU: Maximum Transmission Unit. The default value is 1492. Don’t modify the default value unless necessary.

Service Name:

The current PPPoE connection name. Don’t modify the default value unless necessary.

Server Name:

The Server’s name. Don’t modify the default value unless necessary.

Connect Automatically:

When the device is powered on or disconnected, it connects automatically.

Connect by manual:

When it is disconnected, connect again by manual.

Connect on Demand:

When the data access the device, connect automatically.

Connect on Fixed Time:

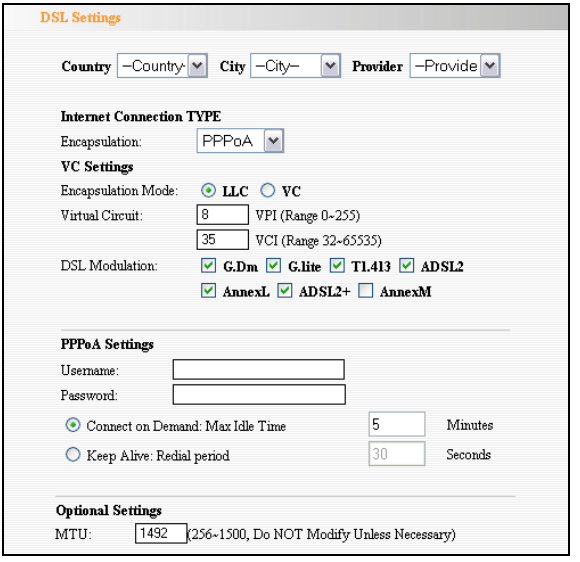
Connect to the Internet on fixed time.

Note:

Only you have set the current time in Time Setting, then "Connect on Fixed Time" can be used.

➔Connection Mode 5：PPPoA

If your ISP provides your connection way as PPPoA, select "PPPoA" in "Encapsulation" field. You need input your user name and password provided by ISP or network administrator in "PPPoA Setting" corresponding fields.



Dial-up Timeout:

During a fixed time, if the auto dial-up fails, the dial-up will stop.

Ideal Timeout:

If there is no communication in the fixed time, the link will be disconnected.

Region selection:

Country, City, Provider. If the city or ISP is not listed in the drop-down menu, you can enter the VPI and VCI value.

"Encapsulation Mode", "DSL Modulation" are suggested to select the default value. If there is something wrong, you can inquire your local ISP.

Other Settings:

MTU: Maximum Transmission Unit. The default value is 1492. Don't modify the default value unless necessary.

Note:

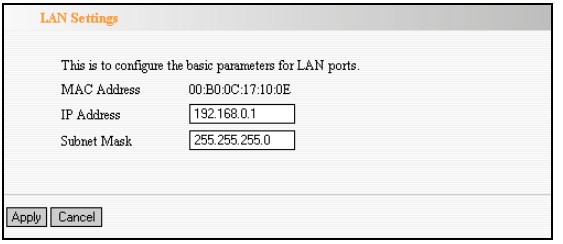
It is recommended using the Setup Wizard to configure the five connection modes: Bridging, MER, IpoA, PPPoE and PPPoA.

Chapter 5：Advanced Setting

This section will guide you to configure the Router's advanced settings, including LAN setting, MAC address clone and DNS setting.

5.1 LAN Setting

This page focuses on how to configure LAN Setting.



MAC Address：

The Router's physical MAC address as seen on your local network, which is unchangeable

IP Address：

The Router's LAN IP address (not your PC's IP address). Once you modify the IP address, you need to remember it for the Web-based Utility login next time. 192.168.0.1 is the default value.

Note:

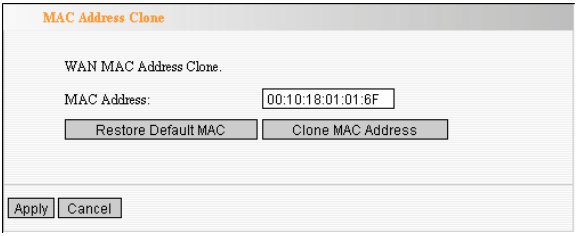
If you have changed the IP address, you need use the new IP address to login the Router's Web interface next time, and the default gateway of all computers in the LAN must be via this IP address to access the Internet.

Subnet Mask:

The Router's subnet mask for measurement of the network size.255.255.255.0 is the default value.

5.2 MAC Address Clone

Some ISPs require end-user's MAC address to access their network. This feature copies the MAC address of your network device to the Router. Input the MAC address to be registered in the field, click "Apply" to implement this feature.



MAC Address:

The MAC address to be registered with your Internet service provider.

Clone MAC Address:

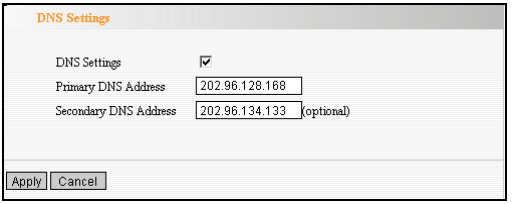
Register your PC's MAC address.

Restore Default MAC Address:

Restore the default hardware MAC address.

5.3 DNS Settings

DNS is short for Domain Name System (or Service), an Internet service that translate domain names into IP addresses which are provided by your Internet Service Provider. Please consult your Internet Service Provider for details if you do not have them.



DNS Setting:

Click the checkbox to enable the DNS server. The Router's DHCP server then will assign the DNS for client's request.

Primary DNS Address:

Enter the necessary address provided by your ISP.

Secondary DNS Address:

Enter the second address if your ISP provides, which is optional.

For example:

Your ISP provides the following address:

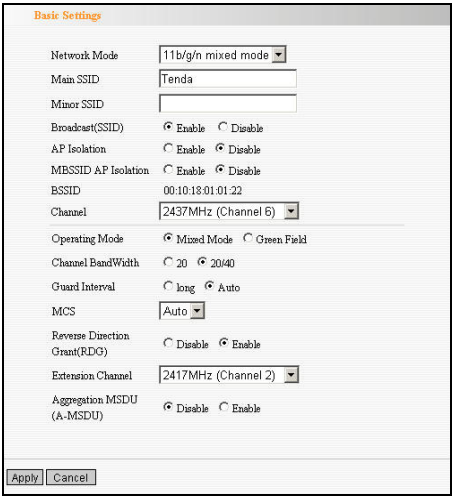
Primary DNS Address: 202.96.128.166

Secondary DNS Address: 202.96.134.133

Chapter 6：Wireless Settings

This section mainly deals with the wireless settings, including Basic Settings, Security Setting, Access Control and Advanced Settings.

6.1 Basic Setting



Network Mode:

Select one mode from the following: 802.11b/g mixed, 802.11b, 802.11g and 802.11b/g/n mixed.

Main SSID：

SSID (Service Set Identifier) is the unique

name of the wireless network. This device has two SSIDs and the main SSID is necessary.

Minor SSID:

Minor Service Set Identifier. It is optional.

Broadcast (SSID):

Select “enable” to enable the device's SSID to be visible by wireless clients.

AP Isolation:

When this feature is enabled, each of your wireless clients will be in its own virtual network and will not be able to communicate with each other. This feature is deployed when you have many guests that frequent your wireless network. For example, configure main SSID as AP1, minor SSID as AP2. PC1 connects to AP1 via wireless adapter; PC2 connecting to AP2. After the feature is enabled, two PCs can not communicate and share network resource each other. (It is essential to enable two SSID before the feature is enabled.) The default AP isolation is disabled.

MBSSID AP Isolation:

When it is enabled, the wireless clients connected with AP can not access each other to isolate completely access control in WLAN.

BSSID:

Business Service Set Identifier of wireless network. In IEEE802.11, BSSID is the MAC address of wireless access point.

Channel:

Specify the effective channel (from 1 to 14) of the wireless network.

Extension Channel:

To increase data throughput of wireless network, the extension channel range is used in 11n mode.

Channel Bandwidth:

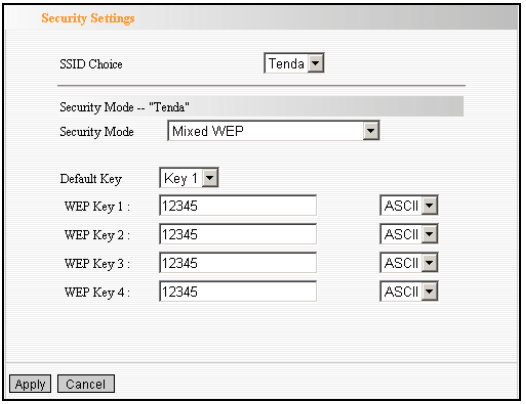
Select channel bandwidth to improve wireless performance. If the wireless network has 11b/g or 11n-compliance, select bandwidth as 40M; if there is no 11n-compliant client, select 20M.

6.2 Wireless Security Settings

This page is used to configure the device's network security setting. Here presents the common six encryption methods, including Mixed WEP, WPA-personal, WPA-enterprise, WPA2-personal, WPA2- enterprise, etc. It is recommended to use WPA2-personal encryption method.

6.2.1 Mixed WEP

WEP (Wired Equivalent Privacy), a basic encryption method, usually encrypts wireless data using a series of digital keys (64 bits or 128 bits in length). By using the same keys on each of your wireless network devices, you can prevent unauthorized wireless devices from monitoring your transmissions or using your wireless resources. WEP is based on RSA algorithm from RC4. It is the original and weak encryption method, so it is recommended not to use this method. Select Mixed WEP to enter the following window:



SSID Choice:

Select the SSID (main SSID or minor SSID) to configure security setting from the drop-down menu.

Security Mode:

From the drop-down menu select the corresponding security encryption modes.

WEP Key:

Set the WEP key with the format of ASCII and Hex.

Key Description:

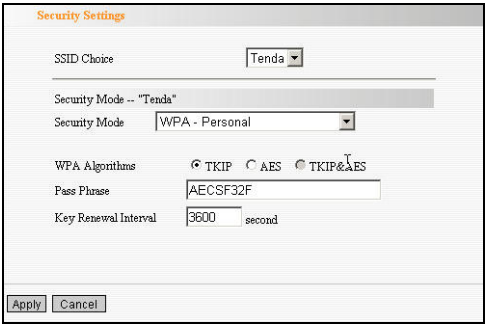
Enter ASCII code (5 or 13 ASCII characters. Illegal character as "/" is not allowed.) or 10/26 hex characters.

Default Key:

Select one key from the four configured keys as the current available one.

6.2.2 WPA- Personal

WPA (Wi-Fi Protected Access), a Wi-Fi standard, is a more recent wireless encryption scheme, designed to improve the security features of WEP. Select “WPA-personal” from the drop-down menu to enter the following window:



WPA Algorithms:

Select one encryption type, AES or TKIP. (AES is stronger than TKIP.)

Pass Phrase:

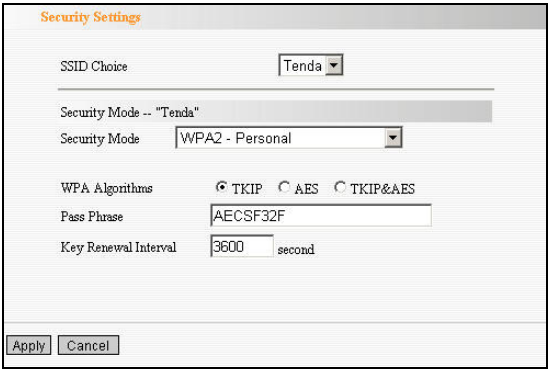
Enter the key which must have 8-63 ASCII characters.

Key Renewal Interval:

Enter the key renewal period. It is to tell the Router how often to change the keys.

6.2.3 WPA2-Personal

WPA2 (Wi-Fi Protected Access version 2), It's more secure than Wired Equivalent Privacy (WEP) and easy to set up.



WPA Algorithms:

Select key Algorithms such as TKIP, AES and TKIP&AES.

Pass Phrase:

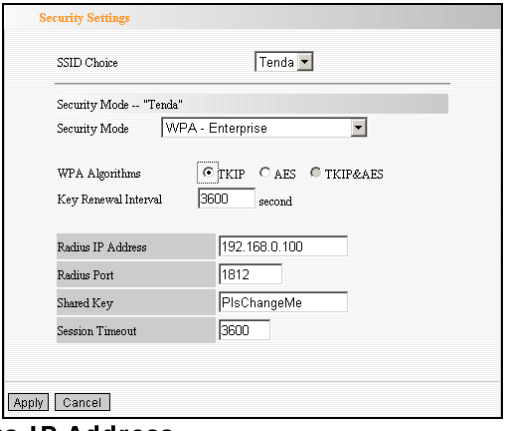
Enter the key which must have 8-63 ASCII characters.

Key Renewal Interval:

Enter the key renewal period. It is to tell the Router how often to change the keys.

6.2.4 WPA-Enterprise

This security mode is used when a RADIUS server is connected to the device. Select “WPA-enterprise” from the drop-down menu to enter the following window:



Radius IP Address:

Enter the IP address of the Radius server.

Radius Port:

Enter the authentication port of the Radius server. The default is 1812.

Shared Key:

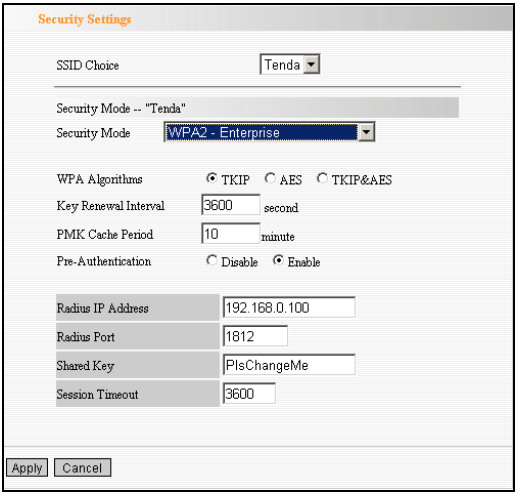
Enter the shared key for authentication server with 8~63 ASCII characters.

Session Timeout:

The authentication interval period between AP and authentication server. The default is 3600s.

6.2.5 WPA2-Enterprise

This security mode is also used when a RADIUS server is connected to the Router.



Radius IP Address:

Enter the IP address of the Radius server.

Radius Port:

Enter the authentication port of the Radius server. The default is 1812.

Shared Key:

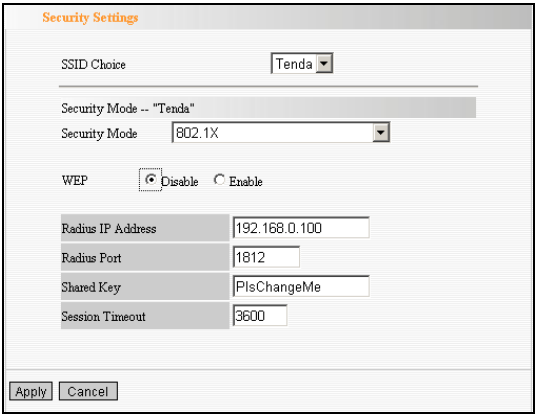
Enter the shared key for authentication server with 8~63 ASCII characters.

Session Timeout:

The authentication interval period between AP and authentication server. The default is 3600s.

6.2.6 802.1X Authentication

This security mode is used when a RADIUS server is connected to the device. 802.1x, a kind of Port-based authentication protocol, is an authentication type and strategy for users. The port can be either a physic port or logic port (such as VLAN). For wireless LAN users, a port is just a channel. The final purpose of 802.11x authentication is to check if the port can be used. If the port is authenticated successfully, you can open this port which allows all the messages to pass. If the port isn't authenticated successfully, you can keep this port "disable" which just allows 802.1x authentication protocol message to pass. Select "802.1x" from the drop-down menu to enter the following window:



WEP:

Click "Enable/Disable" to enable or disable the WEP algorithm.

Radius IP Address:

Enter the IP address of the Radius server.

Radius Port:

Enter the authentication port of the Radius server. The default is 1812.

Shared Key:

Enter the shared key for authentication server with 8~63 ASCII characters.

Session Timeout:

The authentication interval period between AP and authentication server. The default is 3600s.

⚠**NOTE:**

To improve security level, do not use those words which can be found in a dictionary or too easy to remember! Wireless clients will remember the WEP key, so you only have to input the WEP key on wireless client once, and it is worth to use complicated WEP key to improve security level.

6.3 WPS Setting

WPS (Wi-Fi Protected Setting) can be easy and quick to establish the connection between the wireless network clients and the Router through encrypted contents. The users only enter the PIN code to configure without selecting encryption method and entering secret keys by manual.

WPS Config
You could setup security easily by choosing PIN or PBC method to do Wi-Fi Protected Setup.
WPS Settings: Disable Enable
WPS mode: PBC PIN
WPS Summary
WPS Current Status: Not used
WPS Configured: No
WPS SSID: Tenda
WPS Auth Mode: WPA2-PSK
WPS Encryp Type: AES
WPS Default Key Index: 2
WPS Key(ASCII): PleChangeMe
AP PIN: 658263
Save
Reset OOB

WPS Setting：

To enable or disable WPS function. The default is to disable.

WPS Mode：

Supports two ways to configure WPS settings: PBC (Push-Button Configuration) and PIN code

PBC:

Select the PBC or press the WPS button on the front panel of the device for one second (Press the button for one second and WPS indicator will be blinking for 2 minutes, which means the WPS is enabled. During the blinking time, you can enable another device to implement the WPS/PBC negotiation between them. At present, the WPS only supports up to 32 clients access. Two minutes later, the WPS indicator will be off. If more clients are added, repeat the above steps).

PIN:

If this option is enabled, you need to enter a wireless client's PIN code in the field and keep the same code in the client.

WPS Summary:

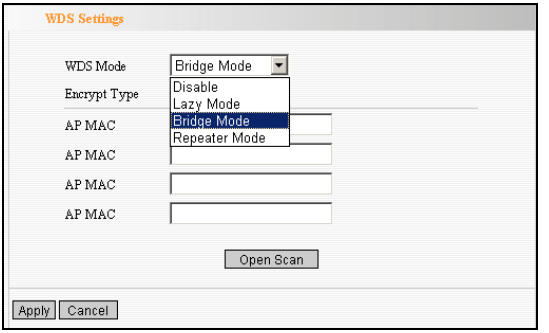
Show Wi-Fi current protection state, authentication mode, encryption method, etc.

⚠ **Note:**

Press the WPS/Reset button for 1 second on the front panel to run PBC. Press for 7 seconds, the device's setting will restore to default setting. The access client has to support WPS function when you implement WPS settings.

6.4 WDS Setting

WDS (Wireless Distribution System) can be used to expand your current wireless network coverage. The Router supports three modes: Lazy, Bridge and Repeater.



Lazy:

In this mode, the connected wireless device should be in Bridge or Repeater mode, and select the Router's BSSID to implement wireless connection.

Bridge:

In this mode, you can connect two or more wired networks via wireless signals. In this mode, you need add the Wireless MAC address of the connecting device into the Router's AP MAC address table or select one from the scanning table.

Repeater:

In this mode, you need add the MAC address of the connecting device into the Router's AP MAC address table to amplify and repeat wireless signals.

Encrypt Type:

You can select WEP mode, TKIP mode, AES mode for security here.

Key:

Enter the encryption key for the connecting devices.

AP MAC Address:

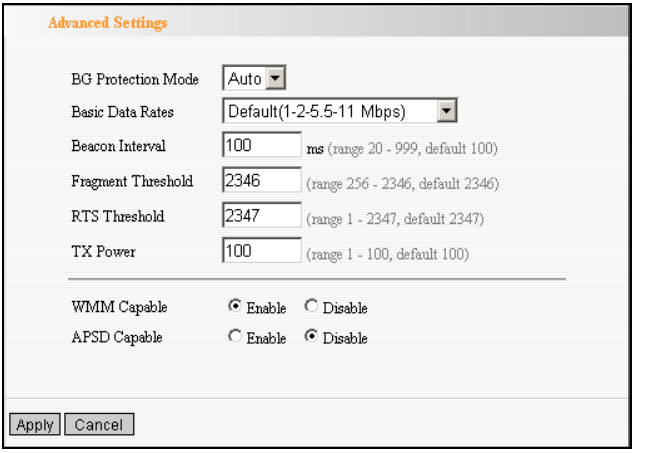
Input the MAC address of the connected wireless device.

⚠**NOTE:**

Two wireless routers must use the same band, channel number, and security settings!

6.5 Advanced Wireless Setting

This section is to configure the advanced wireless setting of the Router, including the Radio Preamble, 802.11g/n Rate, Fragmentation Threshold, RTS Threshold, Beacon Period and DTIM Interval.



BG Protection Mode:

For 11b/g wireless client, it is easier to connect with 11n wireless device. The default is “Auto”.

Basic Data Rates:

In term of different requirements, you can select one of the suitable Basic Data Rates

from the drop-down menu. Here, default value is (1-2-5.5-11Mbps…).

Beacon Interval:

The frequency interval of the beacon, which is a packet broadcast by a router to synchronize a wireless network. The default value is 100 ms. It is recommended not to modify the default value.

Fragment Threshold:

The fragmentation threshold defines the maximum transmission packet size in bytes. The packet will be fragmented if the arrival is bigger than the threshold setting. The default size is 2346 bytes.

RTS Threshold:

RTS stands for “Request to Send”. This parameter controls what size data packet the frequency protocol issues to RTS packet. If the device works in SoHo, do not modify the default value.

TX Power:

Set the wireless output power level. The default value is 100.

WMM Capable:

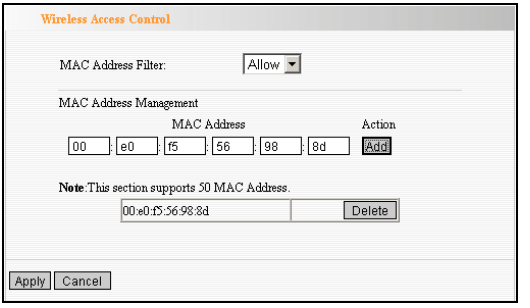
To enhance wireless multimedia transfer performance (0n-line video and voice). If you are not clear about this, enable it.

APSD Capable:

It is used for auto power-saved service. The default is disabled.

6.6 Wireless Access Control

To secure your wireless LAN, the wireless access control is actually based on the MAC address management. Select “Wireless Setting-Access Control” to popup the following window:



MAC Address Filter:

Enable/disable MAC address filter. Select “Off” to malfunction MAC address; “Block” to prevent the MAC addresses in the list from accessing the wireless network; “Allow” to allow the MAC address in the list to access the wireless network.

MAC Address Management:

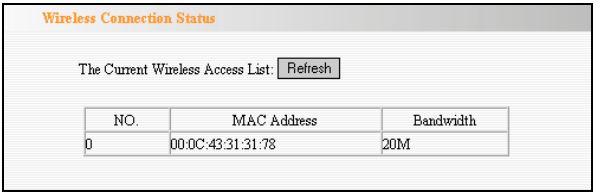
Input the MAC address to implement the filter policy. Click “Add” to finish the MAC adding operation.

MAC Address List:

Show the added MAC address. You can add or delete them.

6.7 Wireless Connection Status

This page is to show the current wireless access status. Click “Refresh” to update the wireless connection information.



MAC Address:

Shows the connecting PC’s MAC address.

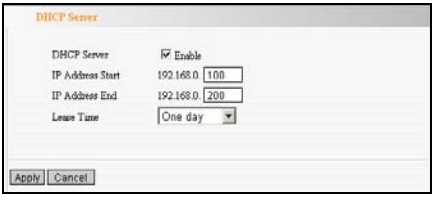
Bandwidth:

Shows the channel bandwidth of the host to be connected.

Chapter 7：DHCP Server

7.1 DHCP Server Setting

DHCP (Dynamic Host Control Protocol) is to assign an IP address to the computers on the LAN/private network. When you enable the DHCP Server, the DHCP Server will allocate automatically an unused IP address from the IP address pool to the requesting computer in premise of activating “Obtain an IP Address Automatically”. So specifying the starting and ending address of the IP Address pool is needed.



DHCP Server:

Activate the checkbox to enable server.

IP Address Start/End:

Enter the range of IP address for DHCP server assignment.

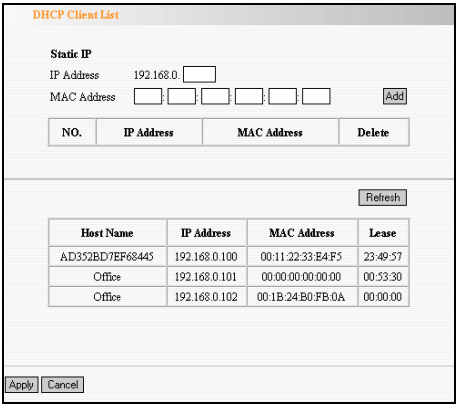
Lease Time:

The time length of the IP address lease.

For example: set the lease time as one hour. Then the DHCP server will recycle and assign the IP address again.

7.2 DHCP Client List

The Static IP assignment is to add one specific static IP address to the assigned MAC address. You can view the related information in the DHCP server list.



IP Address:

Enter one IP address for the computer on the LAN network.

MAC Address:

Enter the MAC address of the computer you want to assign the above IP address. Click “Add” to add the entry in the list.

Hostname:

The name of the computer which is added a new IP address.

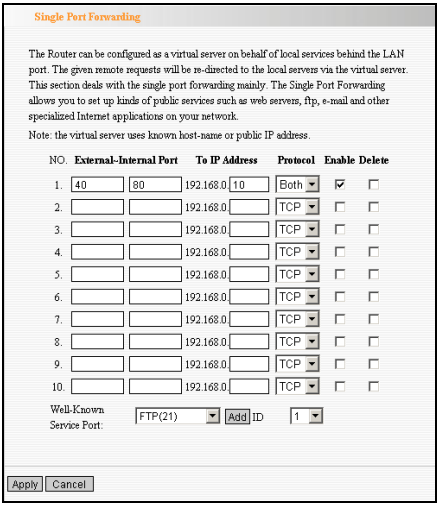
Lease Time:

The time length of the corresponding IP address lease.

Chapter 8：Virtual Server

8.1 Single Port Forwarding

The Router can be configured as a virtual server on behalf of local services behind the LAN port. The given remote requests will be re-directed to the local servers via the virtual server. This section deals with the single port forwarding mainly. The Single Port Forwarding allows you to set up kinds of public services such as web servers, ftp, e-mail and other specialized Internet applications on your network.


Single Port Forwarding
The Router can be configured as a virtual server on behalf of local services behind the LAN port. The given remote requests will be re-directed to the local servers via the virtual server. This section deals with the single port forwarding mainly. The Single Port Forwarding allows you to set up kinds of public services such as web servers, ftp, e-mail and other specialized Internet applications on your network.
Note: the virtual server uses known host-name or public IP address.
NO. External-Internal Port To IP Address Protocol Enable Delete
1. 40 80 192.168.0. 10 Both
2. 192.168.0. TCP
3. 192.168.0. TCP
4. 192.168.0. TCP
5. 192.168.0. TCP
6. 192.168.0. TCP
7. 192.168.0. TCP
8. 192.168.0. TCP
9. 192.168.0. TCP
10. 192.168.0. TCP
Well-Known Service Port: FTP(21) Add ID 1
Apply Cancel

External Port:

This is the external port number for server or Internet application, for example, port 21 for ftp service.

Internal Port:

This is the port number of LAN computer set by the Router. The Internet traffic from the external port will forward to the internal port. For example, you can set the internal port NO.66 to act as the external port NO.21 for ftp service.

IP Address:

Enter the IP address of the PC where you want to set the applications.

Protocol:

Select the protocol (TCP/UDP/Both) for the application.

Enable:

Only click this option to make this rule go into effect.

Delete: To delete this rule.

In Well-known Service Port, list the common ports, you can select one from them and add one ID number from the drop-down menu, click “Add” to add the port in the above table. If the port does not list in the Well-known service port drop-down menu, you can

add it by manual.

Add:

To add the well-know port to ID you selected. If the host with IP address 192.168.0.10 in the LAN provides Web service via port 80, and you want to forward this service to port 40, configure it as the following setting.

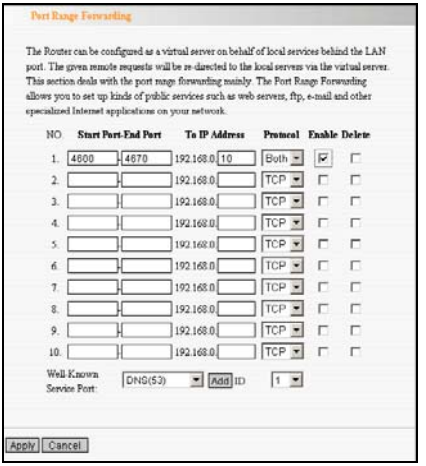
⚠**NOTE**:

If you set the virtual server of the service port as 80, you must set the Web management port on

Remote Web Management page to be any value except 80 such as 8080. Otherwise, there will be a conflict to disable the virtual server.

8.2 Port Range Forwarding

This section deals with the port range forwarding. The Port Range Forwarding allows you to set up a range of public services such as web servers, ftp, e-mail and other specialized Internet applications to an assigned IP address on your LAN.


Port Range Forwarding
The Router can be configured as a virtual server on behalf of local services behind the LAN port. The given remote requests will be re-directed to the local servers via the virtual server. This section deals with the port range forwarding mainly. The Port Range Forwarding allows you to set up kinds of public services such as web servers, ftp, e-mail and other specialized Internet applications on your network.
NO. Start Port-End Port To IP Address Protocol Enable Delete
1. 4600 - 4670 192.168.0. 10 Both
2. 192.168.0. TCP
3. 192.168.0. TCP
4. 192.168.0. TCP
5. 192.168.0. TCP
6. 192.168.0. TCP
7. 192.168.0. TCP
8. 192.168.0. TCP
9. 192.168.0. TCP
10. 192.168.0. TCP
Well-Known Service Port: DNS(53) Add ID 1
Apply Cancel

Start/End Port:

Enter the start/end port number which ranges the External ports used to set the server or Internet applications.

IP Address:

Enter the IP address of the PC where you want to set the applications.

Protocol:

Select the protocol (TCP/UDP/Both) for the application.

Well-Known Service Port:

Select the well-known services as DNS, FTP from the drop-down menu to add to the configured one above.

Delete/Enable:

Click to check it for corresponding operation.

In Well-known Service Port, list the common ports, you can select one from them and add one ID number from the drop-down menu, click “Add” to add the port in the above table. If the port does not list in the Well-known service port drop-down menu, you can add it by manual.

Add: To add the well-know port to ID you selected.

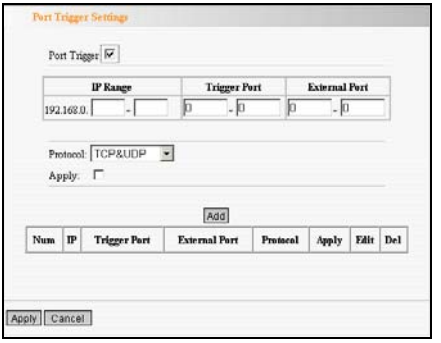
If the host with IP address 192.168.0.10 in the LAN provides Web service via port 80, and you want to forward this service to port 40, configure it as the following setting.

⚠**NOTE:**

If you set the virtual server of the service port as 80, you must set the Web management port on Remote Web Management page to be any value except 80 such as 8080. Otherwise, there will be a conflict to disable the virtual server.

8.3 Port Trigger Setting

When internal clients have access to external server in the Internet for some application, the clients request to connect with severs, and the server will also ask to connect with client. But in the default setting, router will refuse to accept any request from WAN, which will bring communication halt. The port triggering is used to define triggering rules. So when clients have access to the server, the device will open the port through which the server sends the request to client.



IP Range:

The internal IP address range for requesting external server application.

Trigger Port:

The port range through which the internal clients send request traffics to external

server with the range of 1～65535. Note that the low number first and two blanks can keep the same number if needed.

External Port:

The port range through which the external server send request traffics to internal clients with the range of 1～65535. Note that the low number first and two blanks can keep the same number if needed.

Apply:

To enable or disable the rule.

Add:

After edit the rule, click the “add” button to add the current entry to port triggering list.

Apply:

Click “Apply” to activate the current rule.

Cancel:

Click “Cancel” to drop all setting saved last time.

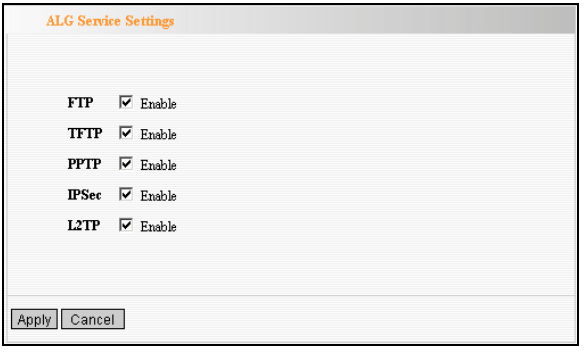
It is allowed to delete or modify the previous rules in the list table.

Note:

The special application can be only used in one PC. If there is more than one PC to open the same triggering port, the external port will be connected to the last PC for the application.

8.4 ALG Service Setting

ALG (Application Layer Gateway) in the context of computer networking, an ALG or application layer gateway consists of a security component that augments a firewall or NAT employed in a computer network. It allows customized NAT traversal filters to be plugged into the gateway to support address and port translation for certain application layer "control/data" protocols such as FTP, Bit Torrent, SIP, RTSP, file transfer applications etc.



In order for these protocols to work through NAT or a firewall, either the application has to know about an address/port number combination that allows incoming packets, or the NAT has to monitor the

control traffic and open up port mappings (firewall pinhole) dynamically as required. Legitimate application data can thus be passed through the security checks of the firewall or NAT that would have otherwise restricted the traffic for not meeting its limited filter criteria.

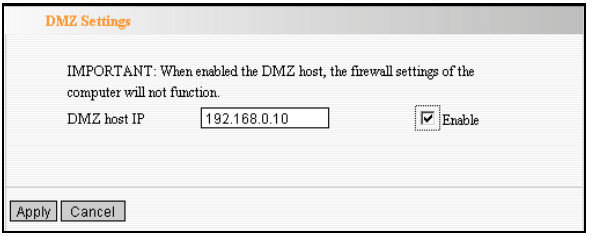
Usually allowing client applications to use dynamic ephemeral TCP/ UDP ports to communicate with the known ports used by the server applications, even though a firewall-configuration may allow only a limited number of known ports. In the absence of an ALG, either the ports would get blocked or the network administrator would need to explicitly open up a large number of ports in the firewall; rendering the network vulnerable to attacks on those ports.

In the default ALG settings, the following protocols have enabled. It is recommended to keep the settings unchanged.

1, FTP
2, TFTP
3, PPTP
4, IPSec
5, L2TP

8.5 DMZ Host

The DMZ function is to allow one computer in LAN to be exposed to the Internet for a special-purpose service as Internet gaming or videoconferencing.



DMZ Host IP Address:

The IP address of the computer you want to expose.

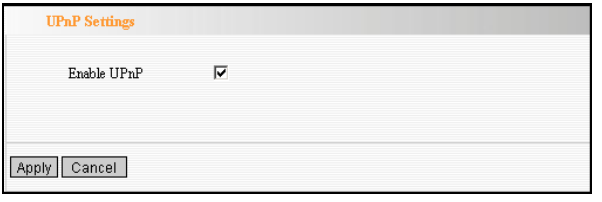
Enable: Click the checkbox to enable the DMZ host.

IMPORTANT:

When enabled the DMZ host, the firewall settings of the DMZ host will not function.

8.6 UPnP Setting

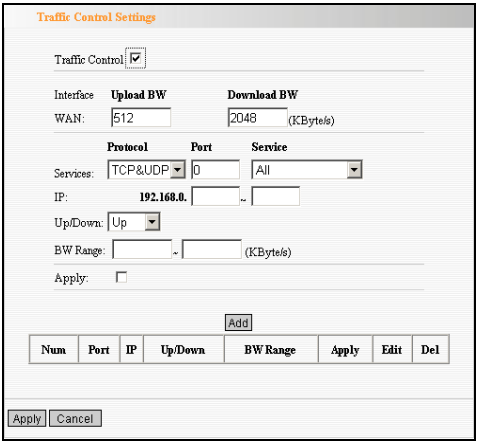
It supports latest Universal Plug and Play. This function goes into effect on Windows XP or Windows ME or this function would go into effect if you have installed software that supports UPnP. With the UPnP function, host in LAN can request the router to process some special port switching so as to enable host outside to visit the resources in the internal host.



Enable UPnP: Click the checkbox to enable the UPnP.

Chapter 9: Traffic Control

Traffic control is used to limit communication speed in the LAN and WAN. Up to 20 entries can be supported with the capability for at most 254 PCs' speed control, including for IP address range configuration.



Enable Traffic Control:

To enable or disable the internal IP bandwidth control.

Interface:

To limit the uploading and downloading bandwidth in WAN port.

Service:

To select the controlled service type, such as

HTTP service.

IP Starting Address:

The first IP address for traffic control.

IP Ending Address:

The last IP address for traffic control.

Uploading/Downloading:

To specify the traffic heading way for the selected IP addresses: uploading or downloading.

Bandwidth:

To specify the uploading/ downloading Min. /Max. traffic speed (KB/s), which can not exceed the WAN speed.

Apply:

To enable the current editing rule. If not, the rule will be disabled.

Add:

After edit the rule, click the “add to list” button to add the current rule to rule list.

Save:

Click “Save” to activate the current rule.

Cancel:

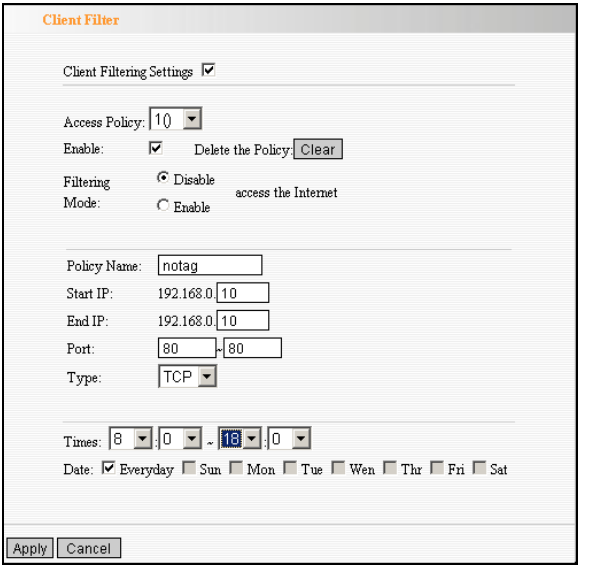
Click “Cancel” to drop all setting saved last time.

It is allowed to delete or modify the previous rules in the list table.

Chapter 10： Security Setting

10.1 Client Filter Settings

To benefit your further management to the computers in the LAN, you can control some ports access to Internet by data packet filter function.



Client Filter:

Check to enable client filter.

Access Policy:

Select one number from the drop-down menu.

Enable:

Check to enable the access policy.

Clear the Policy:

Click “Clear” button to clear all settings for the policy.

Filter Mode:

Click one radio button to enable or disable to access the Internet.

Policy Name:

Enter a name for the access policy selected.

IP Start/End:

Enter the starting/ending IP address.

Port No.:

Enter the port range based over the protocol for access policy.

Protocol:

Select one protocol (TCP/UDP/Both) from the drop-down menu.

Times: Select the time range of client filter.

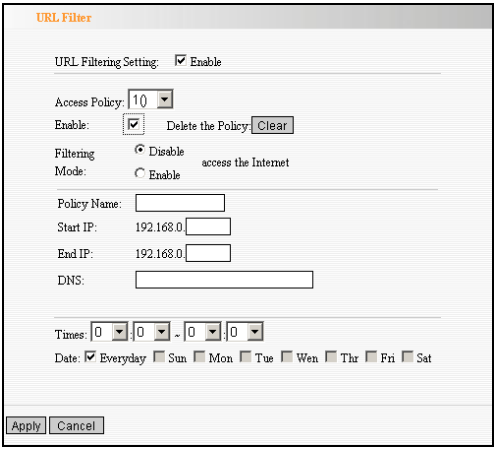
Days: Select the day(s) to run the access policy.

For example:

If you set the IP address 192.168.0.10 not to access the Internet at 8:00-18:00 each day, please configure it as the following page:

10.2 URL Filter

In order to control the computer to have access to websites, you can use URL filtering to allow the computer to have access to certain websites at fixed time and forbids it having access to certain websites at fixed time.



URL Filter: Check to enable URL filter.

Access Policy:

Select one number from the drop-down menu.

Enable:

Check to enable the access policy.

Filter Mode:

Click one radio button to enable or disable to access the Internet.

Policy Name:

Enter a name for the access policy selected.

Start/End IP:

Enter the starting/ending IP address.

URL Strings:

Specify the text strings or keywords in the DNS. If any part of the URL contains these strings or words, the web page will not be accessible and display.

Times:

Select the time range of client filter.

Days:

Select the day(s) to run the access policy.

Apply:

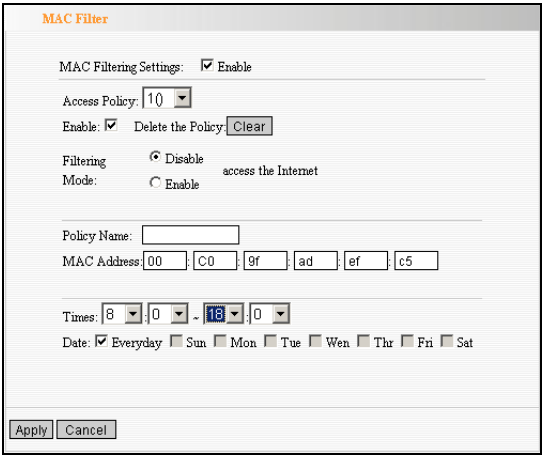
Click to make the settings go into effect.

For example:

if you configure the host with IP address 192.168.0.11 not to access the website containing text strings like “Sex”, please set it as the following page:

10.3 MAC Address Filter

In order to manage the computers in LAN better, you could control the computer's access to Internet by MAC Address Filter.


MAC Filter
MAC Filtering Settings: Enable
Access Policy: 10
Enable: Delete the Policy: Clear
Filtering Mode: Disable Enable access the Internet
Policy Name:
MAC Address: 00 C0 9f ad ef c5
Times: 8 : 0 ~ 18 : 0
Date: Everyday Sun Mon Tue Wen Thr Fri Sat
Apply Cancel

MAC Address Filter:

Check to enable MAC address filter.

Access Policy:

Select one number from the drop-down menu.

Enable:

Check to enable the access policy.

Filter Mode:

Click one radio button to enable or disable to access the Internet.

Policy Name:

Enter a name for the access policy selected.

MAC Address:

Enter the MAC address you want to run the access policy.

Times: Select the time range of client filter.

Days: Select the day(s) to run the access policy.

Apply： Click to make the settings go into effect.

For example:

If you want to configure the host with MAC address 00:C0:9F:AD:FF:C5 not to access the Internet at 8：00-18：00, you need to set it as follows:

10.4 Prevent Network Attack

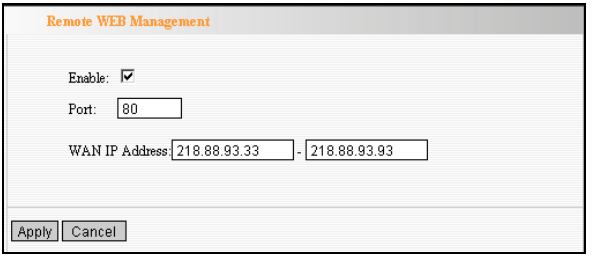
This section is to protect the internal network from exotic attack such as SYN Flooding attack, Smurf attack, LAND attack, etc. Once detecting the unknown attack, the Router will restrict its bandwidth automatically. The attacker's IP address can be found from the "System Log".

Prevent Network Attack:

Check to enable it for attack prevention.

10.5 Remote Web Management

This section is to allow the network administrator to manage the Router remotely. If you want to access the Router from outside the local network, please select the “Enable”.



Enable:

Check to enable remote web management.

Port:

The management port open to outside access. The default value is 80.

WAN IP Address:

Specify the range of the WAN IP address for remote management.

Note:

If you want to login the device’s Web-based interface via port 8080, you need use the format of WAN IP address:

port (for example http://219.134.32.101:8080) to implement remote login.

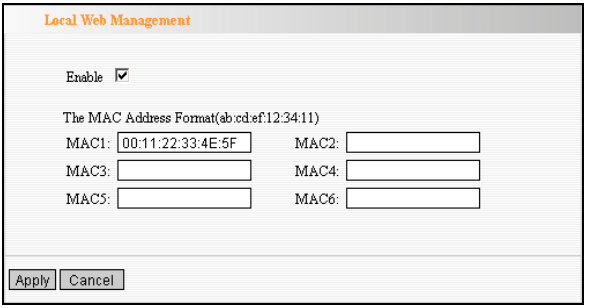
If your WAN IP address starts and ends with 0.0.0.0, it means all hosts in WAN can implement remote Web management. If you change the WAN IP address as 218.88.93.33-218.88.93.35, then only the IP addresses as 218.88.93.33, 218.88.93.34 and 218.88.93.35 can access the Router.

For example:

If you want to configure the IP address 218.88.93.33 to access the device's web interface, please set it as follows:

10.6 Local Web Management

Local web management, the alternative to remote web management, is to allow the network administrator to manage the Router in LAN. Any PC in the LAN can access the Web management utility by default. So you can enter the specific MAC address of the LAN computer to function.



Enable: Check to enable the local web management

MAC1 / 2 / 3…:

Enter the MAC addresses of LAN computers.

Note:

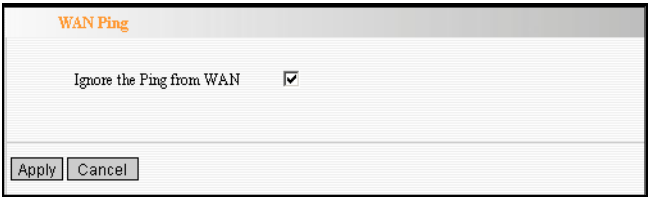
1. In the default state, this feature is not enabled. All computers in the LAN can login the Web.

2. For example, if you only allow the MAC address with 00:11:22:33:E4:F5 to access the Web, please set it as follows.

3. If you just check the frame to enable this feature and not to add any MAC address, all computers can not access the Router's interface via Web.

10.7 WAN Ping

The ping test is to check the status of your internet connection. When disabling the test, the system will ignore the ping test from WAN.



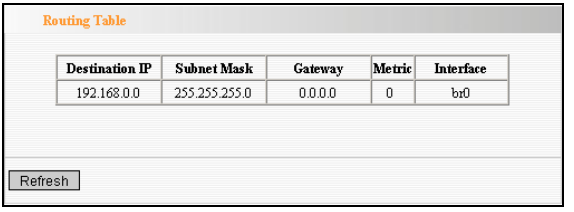
Ignore Ping from WAN:

Check to ignore the ping request and give no reply.

Chapter 11: Routing Setting

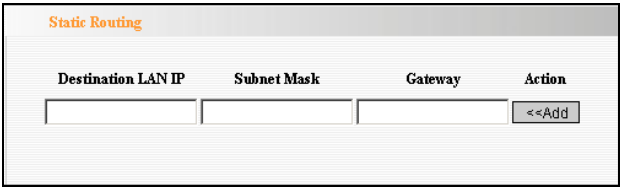
11.1 Routing Table

The main duty for a router is to look for a best path for every data frame, and transfer this data frame to a destination. So, it's essential for the router to choose the best path, i.e. routing arithmetic. In order to finish this function, many transferring paths, i.e. routing table, are saved in the router, for choosing when needed.



11.2 Static Routing

This page is used to configure the Router's static routing.



Destination LAN IP:

The address of the remote host with which you want to construct a static route.

Subnet Mask:

The network portion of the Destination LAN IP.

Gateway:

The gateway of the next hop, usually the Router or host's IP address.

Tip: Static Route is set by system administrator in advance. Usually, It would not be subjected to network structure's change.

Note:

1. The gateway must keep the same segment with the Router's LAN IP address.

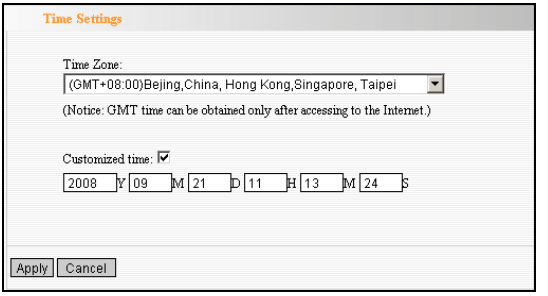
2. If the destination IP address is one host's IP address, the Subnet mask should be 255.255.255.255.

3. If the destination IP address is an IP address range, the subnet mask should match the IP address. For example, if the IP is 10.0.0.0, subnet mask should be 255.0.0.0; if the IP is 10.1.2.0, subnet mask should be 255.255.255.0.

Chapter 12: System Tools

12.1 Time Setting

This section is to select the time zone for your location. If you turn off the Router, the settings for time disappear. However, the Router will automatically obtain the GMT time again once it has access to the Internet.


Time Settings
Time Zone:
(GMT+08:00)Bejing,China, Hong Kong,Singapore, Taipei
(Notice: GMT time can be obtained only after accessing to the Internet.)
Customized time:
2008 Y 09 M 21 D 11 H 13 M 24 S
Apply
Cancel

Time Zone:

Select your time zone from the drop-down menu.

Customized time:

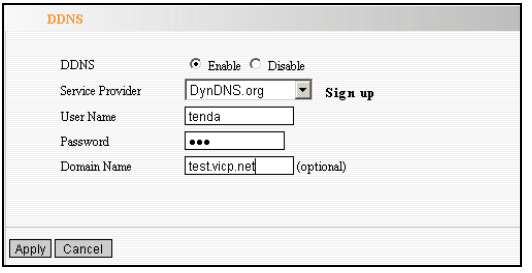
Enter the time you customize.

Note:

When the Router is powered off, the time setting will be lost. Before the Router will obtain GMT time automatically, you need connect with the Internet and obtain the GMT time, or set the time on this page first. Then the time in other features (e.g. firewall) can be go into effect.

12.2 DDNS

The DDNS (Dynamic Domain Name System) is supported in this router. It is to assign a fixed host and domain name to a dynamic Internet IP address, which is used to monitor hosting website, FTP server and so on behind the Router. If you want to activate this function, please select “Enable” and a DDNS service provider to sign up.



DDNS:

Click the radio button to enable or disable the DDNS service.

Service Provider:

Select one from the drop-down menu and press “Sign up” for registration.

User Name:

Enter the user name the same as the registration name.

Password:

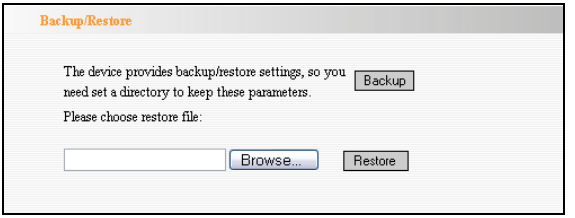
Enter the password you set.

Domain Name:

Enter the domain name which is optional.

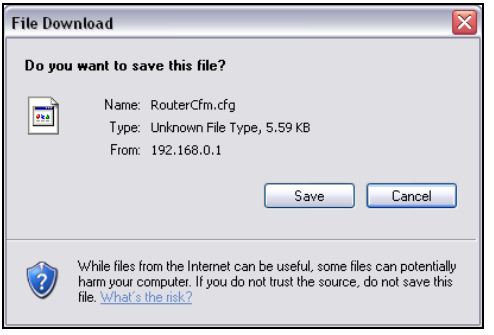
12.3 Backup/Restore Setting

The device provides backup/restore settings, so you need set a directory to keep these parameters.



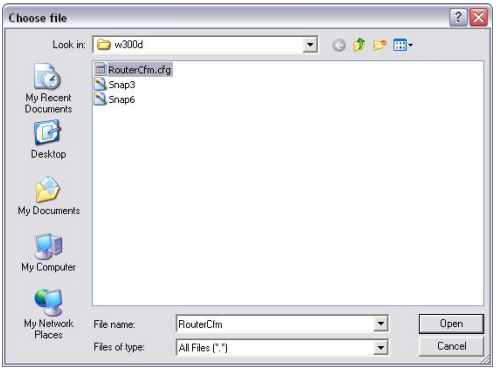
Backup Setting

Click “Backup” button to back up the Router’s settings and select the path for save.

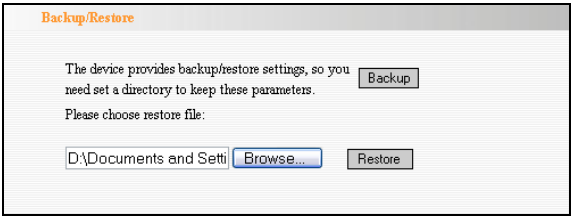

File Download
Do you want to save this file?
Name: RouterCfm.cfg
Type: Unknown File Type, 5.59 KB
From: 192.168.0.1
Save
Cancel
While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not save this file. What's the risk?

Restore Setting:

Click “Browse” button to select the backup files.

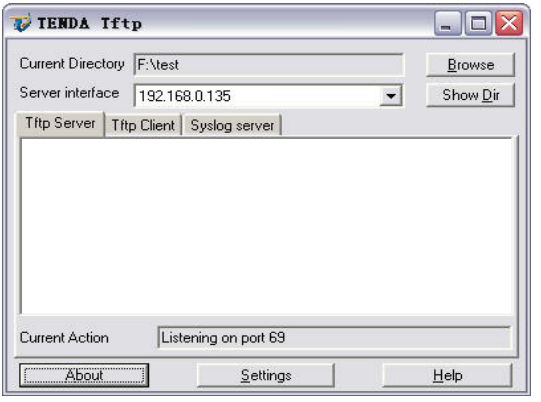


Click “Restore” button to restore previous settings.

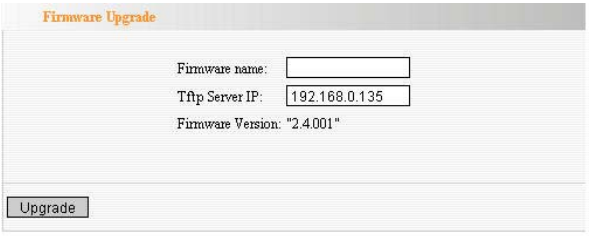


12.4 Firmware Upgrade

The Router provides the firmware upgrade by clicking the “Upgrade” after browsing the firmware upgrade packet which you can download from www.tenda.cn. After the upgrade is completed, the Router will reboot automatically.



Through upgrading the Router’s software, you can gain more stable performance and value-added features. You can download the latest upgrade file and TFTP Server from the website www.tenda.cn. After the upgrade file is downloaded, put the de-condensed upgrade files and TFTP in same directory file.



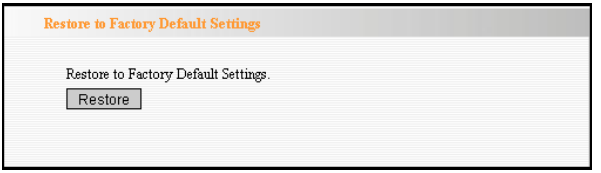
When your computer connects with the Router's LAN port, and obtain the IP address assigned by the Router, please run the TFTP Server, and keep the "Firmware File Name" same with the upgrade file name. Click "Upgrade" to start the firmware upgrading.

IMPORTANT:

Do not power off the system during the firmware upgrade to avoid damaging the device. The Router will reboot after the upgrade.

12.5 Restore to Factory Default Settings

This button is to reset all settings to the default values. It means the Router will lose all the settings you have set. So please Note down the related settings if necessary.



Restore:

Click this button to restore to default settings.

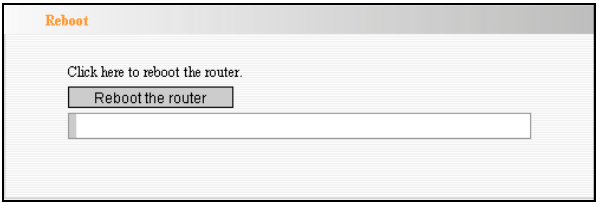
Factory Default Settings:
User Name: admin
Password: admin
IP Address: 192.168.0.1
Subnet Mask: 255.255.255.0

⚠ **NOTE:**

After restoring to default settings, please restart the device, then the default settings can go into effect.

12.6 Reboot

Rebooting the Router makes the settings configured go into effect or to set the Router again if setting failure happens.

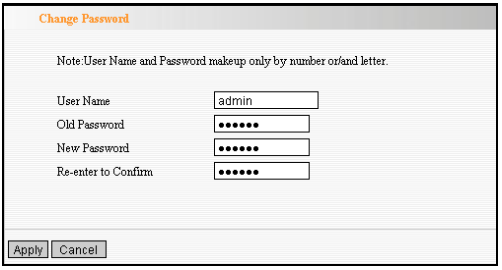


Reboot the router:

Click this button to reboot the device.

12.7 Password Change

This section is to set a new user name and password to better secure your router and network.



User Name:

Enter a new user name for the device.

Old Password:

Enter the old password.

New Password:

Enter a new password.

Re-enter to Confirm:

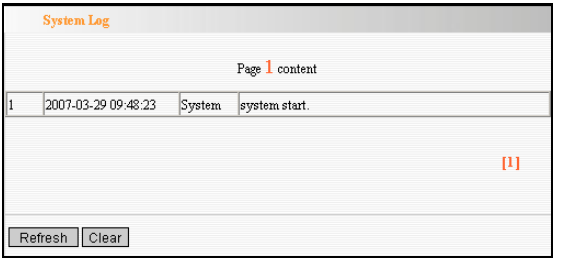
Re-enter to confirm the new password.

⚠**NOTE:**

It is highly recommended to change the password to secure your network and the Router.

12.8 System Log

The section is to view the system log. Click the "Refresh" to update the log. Click "Clear" to clear all shown information. If the log is over 150 records, it will clear them automatically.



Refresh:

Click this button to update the log.

Clear:

Click this button to clear the current shown log.

Appendix I: Glossary

Access Point (AP):

Any entity that has station functionality and provides access to the distribution services, via the wireless medium (WM) for associated stations.

Channel:

An instance of medium use for the purpose of passing protocol data units (PDUs) that may be used simultaneously, in the same volume of space, with other instances of medium use(on other channels) by other instances of the same physical layer (PHY),with an acceptably low frame error ratio(FER) due to mutual interference.

SSID:

Service Set identifier. An SSID is the network name shared by all devices in a wireless network. Your network's SSID should be unique to your network and identical for all devices within the network. It is case-sensitive and must not exceed 20 characters (use any of the characters on the

keyboard).Make sure this setting is the same for all devices in your wireless network.

WEP:

Wired Equivalent Privacy (WEP) is the method for secure wireless data transmission. WEP adds data encryption to every single packet transmitted in the wireless network. The 40bit and 64bit encryption are the same because of out 64 bits, 40 bits are private. Conversely, 104 and 128 bit are the same. WEP uses a common KEY to encode the data. Therefore, all devices on a wireless network must use the same key and same type of encryption. There are 2 methods for entering the KEY; one is to enter a 16-bit HEX digit. Using this method, users must enter a 10-digit number (for 64-bit) or 26-digit number (for 128-bit) in the KEY field. Users must select the same key number for all devices. The other method is to enter a text and let the computer generate the WEP key for you. However, since each product use different method for key generation, it might not work for different products. Therefore, it

is NOT recommend using.

WPA/WPA2:

A security protocol for wireless networks that builds on the basic foundations of WEP. It secures wireless data transmission by using a key similar to WEP, but the added strength of WPA is that the key changes dynamically. The changing key makes it much more difficult for a hacker to learn the key and gain access to the network.WPA2 is the second generation of WPA security and provides a stronger encryption mechanism through Advanced Encryption Standard (AES), which is a requirement for some government users.

ADSL:

Short for Asymmetric Digital Subscriber Line -- A method for moving data over regular phone lines. An ADSL circuit is much faster than a regular phone connection, and the wires coming into the subscriber's premises are the same (copper) wires used for regular phone service. A commonly discussed configuration of ADSL would allow a subscriber to receive data (download) at speeds of up to 1.544 megabits (not

megabytes) per second, and to send (upload) data at speeds of 128 kilobits per second. Thus the "Asymmetric" part of the acronym.

ATM：

ATM stands for Asynchronous Transfer Mode. A transmission protocol that breaks down user traffic into small fixed-sized cells, before reassembling them after transmission. During transmission, cells from different users are asynchronously intermixed, thereby maximizing network resources. The ATM advantages voice and video stream and data transmission in single network.

VPI：

Stands for "Virtual Path Identifier." The VPI is an 8-bit header inside each ATM cell that indicates where the cell should be routed. It is used to identify the virtual path (a bundle of virtual channels that have the same endpoint) to which the cell belongs as it travels through an ATM network. As an ATM cell moves across a network, it typically passes through several ATM switches. The VPI tells the switches where to route the packet of information, or what path to take.

Hence the name, "virtual path identifier." The VPI is used in conjunction with the VCI, or virtual channel identifier.

VCI：

Stands for "Virtual Channel Identifier." The VCI indicates where an ATM cell is to travel over a network. The VCI within each ATM cell defines the fixed channel on which the packet of information should be sent. It is a 16-bit field, compared to the VPI, which is only 8 bits. Since this numerical tag specifies the virtual channel that each packet belongs to, it prevents interference with other data being sent across the network.

Bridging：

Here is related to the well-known RFC1483 bridging protocol. This feature is working on the basic bridging protocol and physical layer. In this device, Modem serves as a bridge device, and does not provide any protocol transfer and address filtering features. In this case, the Modem actually plays the role as Hub.

IPoA：

It is related to RFC1577. Usually the data

packets are transferred via ATM network. In this connection mode, user must have static IP address, subnet mask and other parameters. Lack of user name and password authentication, it can not implement network administration and QoS features, so this access way will not prevail any more.

PPPoA:

Short for Point-to-Point Protocol over Asynchronous Transfer Mode (ATM). PPPoA relies on two widely accepted standards: PPP and ATM. It is an end-to-end asymmetric digital subscriber line (ADSL) architecture. IP packets travel from the PC over Ethernet to the DSL modem, called the ADSL transceiver unit-remote (ATU-R). The ATU-R adds the PPP protocol to the IP packets and transports them to the carrier's Digital Subscriber Line Access Multiple (DSLAM) via ATM. It is a technology becoming more popular with DSL providers.

PPPoE:

Acronym for Point-to-Point Protocol over Ethernet. PPPoE relies on two widely accepted standards: PPP and Ethernet.

PPPoE is a specification for connecting the users on an Ethernet to the Internet through a common broadband medium, such as a single DSL line, wireless device or cable modem. All the users over the Ethernet share a common connection, so the Ethernet principles supporting multiple users in a LAN combine with the principles of PPP, which apply to serial connections.